GEORGETOWN LAW
INSTITUTE FOR PUBLIC REPRESENTATION

Directors
Hope M. Babcock
Aderson Francois
Laura M. Moy
Benton Senior Counselor
Andrew Jay Schwartzman
Staff Attorneys
Yael Bromberg*
Peter DeMarco
Sarah Fox
Patrick Llewellyn
Drew T. Simshaw

600 New Jersey Avenue, NW, Suite 312
Washington, DC 20001-2075
Telephone: 202-662-9535
Fax: 202-662-9634

September 27, 2016

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12 St. SW
Washington, DC 20554

Re: WC Docket No. 16-106, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*; WC Docket No. 13-306, *Petition of Public Knowledge et al. for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent*

Dear Ms. Dortch:

On Monday, September 26, Sarah Morris and Eric Null of New America's Open Technology Institute, together with their counsel, Laura Moy of the Institute for Public Representation at Georgetown Law (collectively, "OTI"), met with Gigi Sohn and Ruth Milkman of the Chairman's office, and Matt DelNero and Lisa Hone of the Wireline Competition Bureau, to discuss matters in the above-referenced proceedings.

Carving Out De-Identified Customer Data

OTI argued, as it has in the past, that supposedly de-identified customer information should only be regulated separately from customer proprietary information or individually identifiable customer proprietary network information if it meets the statutory definition of aggregate customer information under 47 U.S.C. § 222, that is, that it is "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." Thus, information that has merely been pseudonymized (i.e. purged of datapoints typically considered to be personally identifying, but with the data largely left intact) would not meet the definition of aggregate customer information for two reasons: because it would not be "collective data," and because it would not have been purged of individual customer "characteristics." BIAS providers would not be barred from using pseudonymized information or information that otherwise has been de-identified in a manner that does not meet the definition of aggregate customer information, they would simply need to obtain their customers' affirmative opt-in consent to use such data for non-service-related purposes.

On the other hand, the FCC could find that certain de-identification techniques are allowable without prior opt-in customer consent if those techniques meet the definition of aggregate customer information under the statute. As defined in the statute, "aggregate customer information" is "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." So, for example, "aggregate customer information" may well encompass attributes regarding a customer dataset that have been extracted through meaningfully implemented differential privacy, where individual characteristics are therefore never revealed.

Carefully Limiting the Non-Service-Related Purposes for Which BIAS Providers May Use Customer Information on an Opt-Out Basis

OTI reiterated its support for the FCC's proposal to carefully cabin the extent to which BIAS customers' information can be used for non-service-related purposes on an opt-out basis. In initial comments, OTI argued that the FCC should limit an opt-out allowance to situations in which customer information would be used to advertise

telecommunications, cable, and/or satellite services regulated by the FCC.[1] In that context, OTI explained that allowing the use of customer information for advertising on an opt-out basis for other products "could raise competitive concerns."[2] In OTI's paper on *The FCC's Role in Protecting Online Privacy*, OTI described the competitive concerns raised by allowing BIAS providers to use their customer information for marketing of unrelated services:

ISPs' role as Internet gatekeepers also enables them to obtain intimate insight into the otherwise confidential details of other companies' dealings with their customers, including companies that compete directly with the ISP and its affiliates in other markets. For example, AT&T, which markets its own version of a home security system, could use its position as an ISP to surveil private business communications that pass between its subscribers and a home security company that competes with AT&T in that market. It might elect, for example, to track which users seek technical support on the competitor's site, and extend special offers to those users. Such behavior—which is technically feasible— could gravely undermine the Internet's effectiveness as an open engine of commerce. It also runs counter to the basic expectations that Congress, businesses, and consumers have of common carriers entrusted with maintaining the key communications infrastructure of the 21st century.[3]

If the FCC is going to allow BIAS providers to use customer information on an opt-out basis to market the other services they provide, the FCC should strictly cabin such an allowance to marketing related to other communications services regulated by the FCC.

Drawing a Distinction Between "Sensitive" and "Non-Sensitive" Customer Information

OTI reiterated arguments previously made in this docket that it would be inadministrable and unwise for the FCC to offer less protection to customer information it considers "non-sensitive." Many consumer advocates have expressed skepticism that BIAS providers could effectively and reliably parse the sensitive from the non-sensitive

[1] Comments of OTI at 26.
[2] *Id.*
[3] New America's Open Technology Institute, *The FCC's Role in Protecting Online Privacy: An Explainer* 2016 at 6, https://static.newamerica.org/attachments/12325-the-fccs-role-in-protecting-online-privacy/CPNI__web.d4fbdb12e83f4adc89f37ebffa3e6075.pdf.

without in some way examining datasets to determine whether they contain sensitive information. Moreover, sensitive information can be extracted from data that might not immediately appear to be sensitive. For example, as OTI has previously explained, a BIAS provider could analyze traffic patterns to learn information about when a customer is home or away, and when one's daily routine changes dramatically, for example due to a change in employment or family status.[4] By taking into account MAC addresses of smart home devices connected to the network and the traffic patterns of those devices, a BIAS provider could learn even more intimate details about a customer's private life.[5]

Offering Financial Inducements for Certain Privacy Elections

OTI argued that the FCC should look closely and critically at financial incentives offered by companies to induce customers to make certain privacy choices. For individuals with limited financial resources, a financial "incentive" for a particular privacy-intrusive plan could have the effect of erecting a financial barrier that forecloses privacy protective options, especially when the price differential is significant. The FCC should ensure these practices do not become prevalent by making clear they are unacceptable under Section 201(b) of the Communications Act.

Respectfully submitted,

/s/

Laura M. Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9547

Counsel for New America's Open Technology Institute

[4] *Id.* at 5–6.
[5] *Id.* at 6.